ON ARITHMETIC PROGRESSIONS ON EDWARDS CURVES

ENRIQUE GONZÁLEZ–JIMÉNEZ

Abstract. Let be $m \in \mathbb{Z}_{>0}$ and $a, q \in \mathbb{Q}$. Denote by $\mathcal{AP}_m(a,q)$ the set of rational numbers d such that $a, a+q, \dots, a+(m-1)q$ form an arithmetic progression in the Edwards curve $E_d : x^2+y^2 = 1 + d\,x^2y^2$. We study the set $\mathcal{AP}_m(a,q)$ and we parametrize it by the rational points of an algebraic curve.

1. Introduction

Let $F(x,y) \in \mathbb{Q}[x,y]$ be a polynomial in two variables such that its locus defines a plane model of an elliptic curve E over $\mathbb{Q}$. Let $x_1, \dots, x_n$ be an arithmetic progression of rational numbers, we say that $x_1, \dots, x_n$ in $E(\mathbb{Q})$ if they are the x-coordinates of $P_1, \dots, P_n \in E(\mathbb{Q})$. If this happens, we also say that $P_1, \dots, P_n$ is an arithmetic progression in $E(\mathbb{Q})$. Several authors [6, 10, 12, 13, 2, 20, 17, 15, 7, 21, 22, 16, 1, 18, 19] have studied this problem depending on the shape of the polynomial $F(x,y)$. Moreover, some of them have worked with the y-coordinates instead of the x-coordinates. There is an important difference in function of the shape of the polynomial $F(x,y)$. If the polynomial $F(x,y)$ is symmetric in both variables then there is no difference between studying the points with respect to x-coordinates and y-coordinates. This happens in the case of the so called Edwards curves, that is, when $F(x,y) = x^2+y^2-1-dx^2y^2$ for some $d \in \mathbb{Q}$, $d \neq 0, 1$. We denote by E_d such elliptic curve. These curves have been deeply studied in cryptography and it has been found that the resulting addition formulas are very efficient, simple and symmetric (for instance, without distinction of addition and doubling).

In this paper we fix our attention on Edwards curves. The starting point of this work is Moody's paper [18] where he studied the case $0, \pm 1, \pm 2, \pm 3, \dots$; proving that there are infinitely many choices of d such that $0, \pm 1, \pm 2, \pm 3, \pm 4$ form an arithmetic progression in $E_d(\mathbb{Q})$. At the end of his paper, he wondered if this arithmetic progression could be longer. Then he tried, by computer search, to find if a rational d exists with the extra requirement that ± 5 belongs to the arithmetic progression too. He did not succeed and stated that it is an open problem to find an Edwards curve with an arithmetic progression of length 10 or longer. Our first objective was to prove that a rational d such that $0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5$ form an arithmetic progression in $E_d(\mathbb{Q})$ does not exist. Although we will not answer Moody's question we will try to convince the reader that the maximum possible length of an arithmetic progression in an Edwards curve is 9.

Date: April 17, 2013.

2010 *Mathematics Subject Classification.* Primary: 11G05, 11G30; Secondary: 11B25, 11D45, 14G05.

Key words and phrases. Arithmetic progression, Elliptic curves, Edwards curves.

The author was partially supported by the grant MTM2012–35849.

Let $m \in \mathbb{Z}_{>0}$, $a, q \in \mathbb{Q}$ be such that $q > 0$, and denote by

$$\mathcal{AP}_m(a,q) = \{d \in \mathbb{Q} \,|\, a, a+q, a+2q, \dots, a+(m-1)q \text{ in } E_d(\mathbb{Q})\}.$$

Note that if $q < 0$ and $a + nq$ in $E_d(\mathbb{Q})$ then $-a + n(-q)$ in $E_d(\mathbb{Q})$. Therefore, we can assume without loss of generality that $q > 0$.

Let us restrict for a moment to the case of symmetric progressions, that is if an element belongs to the sequence then its negative does. Two possibilities exist: $a = 0$ (central) and $a = \pm q/2$ (non-central). Note that if $0, q, \dots, mq$ in $E_d(\mathbb{Q})$, then $-q, \dots, -mq$ in $E_d(\mathbb{Q})$ too. Therefore we denote by

$$\mathcal{S}_c\mathcal{AP}_{2m+1}(q) = \mathcal{AP}_{2m+1}(-mq, q).$$

Similarly, if $q/2, 3q/2 \dots, (2m-1)/2q$ in $E_d(\mathbb{Q})$, then $-q/2, -3q/2 \dots, -(2m-1)/2q$ in $E_d(\mathbb{Q})$ too. Then we denote by

$$\mathcal{S}_{nc}\mathcal{AP}_{2m}(q) = \mathcal{AP}_{2m}(-(2m-1)q/2, q).$$

Therefore if we denote by $\mathcal{SAP}_m$ the set of rationals d such that a symmetric arithmetic progression of length m belongs to $E_d(\mathbb{Q})$, we have

$$\mathcal{SAP}_m(q) = \begin{cases} \mathcal{S}_c\mathcal{AP}_m(q) & \text{if } m \text{ is odd,} \\ \mathcal{S}_{nc}\mathcal{AP}_m(q) & \text{if } m \text{ is even.} \end{cases}$$

Theorem 1. (Non-Symmetric Case) *Let $m \in \mathbb{Z}_{>0}$ and $a, q \in \mathbb{Q}$ be such that $q > 0$ and (a,q) does not correspond to a symmetric arithmetic progression. Then*

- *$\#\mathcal{AP}_m(a,q) = \infty$ if $m \leq 3$, except for maybe a finite number of pairs (a,q).*
- *$\#\mathcal{AP}_4(a,q) = \infty$ if and only if $a + kq \in \{\pm 1\}$ for some $k \in \{0,1,2,3\}$.*
- *$\#\mathcal{AP}_5(a,q) = \infty$ if and only if $(a,q) \in \left\{\left(1, \frac{2}{3}\right), \left(1, \frac{1}{2}\right), \left(\frac{5}{3}, \frac{2}{3}\right), (5,2), (3,1), (7,2)\right\}$.*
- *If $m \geq 6$ and $(a,q) \in \left\{\left(1, \frac{2}{3}\right), \left(1, \frac{1}{2}\right), \left(\frac{5}{3}, \frac{2}{3}\right), (5,2), (3,1)\right\}$, then $\#\mathcal{AP}_m(a,q) = 0$.*

Theorem 2. (Central Symmetric Case) *Let $m \in \mathbb{Z}_{>0}$ and $q \in \mathbb{Q}_{>0}$ be such that m is odd. Then:*

- *$\#\mathcal{S}_c\mathcal{AP}_m(q) = \infty$ if $m \leq 7$.*
- *$\#\mathcal{S}_c\mathcal{AP}_9(q) = \infty$ if and only if $q \in \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}\right\}$.*
- *If $m \geq 11$ and $q \in \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}\right\}$, then $\#\mathcal{S}_c\mathcal{AP}_m(q) = 0$.*

Theorem 3. (Non-Central Symmetric Case) *Let $m \in \mathbb{Z}_{>0}$ and $q \in \mathbb{Q}_{>0}$ be such that m is even. Then:*

- *$\#\mathcal{S}_{nc}\mathcal{AP}_m(q) = \infty$ if $m \leq 6$.*
- *$\#\mathcal{S}_{nc}\mathcal{AP}_8(q) = \infty$ if and only if $q \in \left\{2, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}\right\}$.*
- *If $m \geq 10$ and $q \in \left\{2, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}\right\}$, then $\#\mathcal{S}_{nc}\mathcal{AP}_m(q) = 0$.*

On section 6 we performed a computer search to find q such that $\mathcal{SAP}_m(q)$ is non-empty for $m \geq 10$. But we did not succeed. Then we left the following questions to the reader:

Question. *Is 9 the maximum length of an arithmetic progression on an Edwards curve? In other words, is $\#\mathcal{AP}_m(a,q) = 0$ for any pair a, q and $m \geq 10$?*

2. Arithmetic-Algebraic-Geometric translation.

Let $d \in \mathbb{Q}$ be such that $d \neq 0, 1$. Then the Edwards curve is the elliptic curve defined by

$$E_d :\, x^2 + y^2 = 1 + d\, x^2 y^2.$$

We have that $(\pm 1, 0), (0, \pm 1) \in E_d(\mathbb{Q})$ (trivial points in the sequel). Moreover, since the model defined above is symmetric if $(x, y) \in E_d(\mathbb{Q})$ then $(\pm x, \pm y), (\pm y, \pm x) \in E_d(\mathbb{Q})$.

Let $(x, y) \in E_d(\mathbb{Q})$ be a non-trivial point, then we can recover d from (x, y):

$$d(x, y) = \frac{x^2 + y^2 - 1}{x^2 y^2}.$$

Assume that this point is of the form $(x, y) = \left(a + nq, \frac{w}{z_n}\right)$, where $n \in \mathbb{Z}_{\geq 0}$, $a, q \in \mathbb{Q}$ such that $q \neq 0$. Then we define

$$d_n := d\left(a + nq, \frac{w}{z_n}\right) = \frac{w^2 + z_n^2((a + nq)^2 - 1)}{(a + nq)^2 w^2}.$$

Notice that $a + nq \neq 0, \pm 1$ and $w \neq \pm z_n$ (resp. $n, q, w \neq 0$) since $d_n \neq 0, 1$ (resp. the point is non-trivial).

Now, let be $\mathcal{S} = \{n_0, \dots, n_{m-1}\} \subset \mathbb{Z}_{\geq 0}$. Then the finite set of equations

$$\mathcal{C}_{\mathcal{S}}^{a,q} \;:\; \{d_i = d_j \mid i, j \in \mathcal{S}\}$$

define a curve in $\mathbb{P}^m$, where the points are $[w : z_0 : \cdots : z_{m-1}]$. Moreover, it is easy to check that a model of this curve may be obtained by fixing one element of $\mathcal{S}$, say n_0, and varying the rest of the elements of the set $\mathcal{S}$:

$$\begin{aligned}\mathcal{C}_{\mathcal{S}}^{a,q} \;:\; \{(n_0 - n_j)q(2a + q(n_0 + n_j))w^2 + (a + n_j q)^2(1 - (a + n_0 q)^2)z_{n_0}^2 &= \\ (a + n_0 q)^2(1 - (a + n_j q)^2)z_{n_j}^2\}_{j=1,\dots,m-1}&\end{aligned}$$

That is, $\mathcal{C}_{\mathcal{S}}^{a,q}$ is the intersection of $m - 1$ quadric hypersurfaces in $\mathbb{P}^m$ and therefore its genus is $(m - 3)2^{m-2} + 1$ (cf. [14, Prop. 4] or [3]). Moreover, the points $[1 : \pm 1 : \cdots : \pm 1] \in \mathcal{C}_{\mathcal{S}}^{a,q}$ correspond to the not-allowed case $d = 1$. Therefore we have the following bijection:

$$\left\{\left(a + n_i q, \frac{w}{z_{n_i}}\right) \in E_d(\mathbb{Q}) \smallsetminus \{(\pm 1, 0), (0, \pm 1)\} \;\middle|\; n_i \in \mathcal{S}\right\} \leftrightarrow \mathcal{C}_{\mathcal{S}}^{a,q}(\mathbb{Q}) \smallsetminus \{[\pm 1 : \cdots : \pm 1]\}.$$

We are going to rewrite the equations of $\mathcal{C}_{\mathcal{S}}^{a,q}$. For this purpose, for any $i, j, k \in \mathbb{Z}_{>0}$ we denote

$$s_{ij} = \frac{q(i - j)(2a + (i + j)q)}{(a + iq)^2(1 - (a + jq)^2)}, \qquad r_{ij} = s_{ij}^{-1}, \qquad t_{ijk} = \frac{s_{ik}}{s_{ij}}.$$

Then

$$\mathcal{C}_{\mathcal{S}}^{a,q} \;:\{X_j^2 = a_j X_0^2 + (1 - a_j)X_1^2\}_{j=1,\dots,m-1}$$

where $a_j = s_{n_0 n_j}$, $X_0 = w$ and $X_j = z_{n_j}$ for any $n_j \in \mathcal{S}$.

Now, we parametrize the first equation as

$$[X_0 : X_1 : X_2] = [t^2 - 2t + a_1 : -t^2 + a_1 : t^2 - 2a_1 t + a_1].$$

Using this parametrization we substitute X_0, X_1 in the rest of equations and we obtain a new system of equations of the curve, depending on the parameter t:

$$\mathcal{C}_{\mathcal{S}}^{a,q} \;: \{X_j^2 = t^4 - 4a_j t^3 + 2(-a_1 + 2a_j + 2a_1 a_j)t^2 - 4a_1 a_j t + a_1^2\}_{j=2,\dots,m-1}\,.$$

Notice that each single equation defines an elliptic curve $\mathbb{Q}$-isomorphic to the elliptic curve with Weierstras model

$$\mathcal{C}^{a,q}_{\{n_0,n_1,n_j\}} \,:\, y^2 = x(x+a_1-a_j)(x+a_j(a_1-1)).$$

Where the isomorphism sends $[1:1:1:1]$ to $\mathcal{O}=[0:1:0]$ and if we denote by $P_0=(0,0), P_1=(a_j-a_1,0), Q=(a_j,a_1a_j)$ then it sends the set $\{[\pm1:\pm1,\pm1:\pm1]\}$ to $\{\mathcal{O},P_1,P_2,P_1+P_2,Q,Q+P_1,Q+P_2,Q+P_1+P_2\}$.

Moreover, each pair of equations define a genus five curve $\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}$ such that its jacobian $\mathrm{Jac}(\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}})$ splits completely over $\mathbb{Q}$ as the product of five elliptic curves. To prove the previous assertion let us write $\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}$ as (see [5]):

$$(1) \qquad \mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}} \,:\, \begin{cases} X_2^2 = b_2X_0^2+(1-b_2)X_1^2, \\ X_3^2 = b_3X_0^2+(1-b_3)X_1^2, \\ X_4^2 = b_4X_0^2+(1-b_4)X_1^2, \end{cases}$$

where $X_3=X_i$, $X_4=X_j$ and $b_2=a_1$, $b_3=a_i$, $b_4=a_j$. Then we have five quotients of genus one such that each one is the intersection of two quadric surfaces in $\mathbb{P}^3$. Any elliptic curve $E_{(k)}$ consists of removing the variables X_k from the previous system of equations. We display the Weierstrass model of those elliptic curves together a (in general) non-torsion point on it:

$$\begin{array}{llr}
E_{(4)} & : y^2 = x(x+b_2-b_3)(x+b_3(b_2-1)), & Q_4=(b_3,b_2b_3), \\
E_{(3)} & : y^2 = x(x+b_2-b_4)(x+b_4(b_2-1)), & Q_3=(b_4,b_2b_4), \\
E_{(2)} & : y^2 = x(x+b_3-b_4)(x+b_4(b_3-1)), & Q_2=(b_4,b_3b_4), \\
E_{(1)} & : y^2 = x\left(x+b_2(b_3-b_4)\right)\left(x+b_4(b_3-b_2)\right), & Q_1=(b_2b_4,b_2b_3b_4), \\
E_{(0)} & : y^2 = x\left(x+(b_2-1)(b_3-b_4)\right)\left(x+(b_4-1)(b_3-b_2)\right), & \\
 & & Q_0=((b_4-1)(b_2-1),(b_2-1)(b_3-1)(b_4-1)).
\end{array}$$

Therefore we have obtained $\mathrm{Jac}(\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}) \overset{\mathbb{Q}}{\sim} E_{(0)}\times E_{(1)}\times E_{(2)}\times E_{(3)}\times E_{(4)}$. In general, $\mathrm{rank}_{\mathbb{Z}}\,\mathrm{Jac}(\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}) \geq 5 = \mathrm{genus}(\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}})$. That is, the classical Chabauty's method [11] does not work to obtain $C^{a,q}_{\{n_0,n_1,n_i,n_j\}}(\mathbb{Q})$. But, in a joint work [14] of the author and Xavier Xarles we developed a method based on covering collections and elliptic curve Chabauty techniques to obtain in some case the rational points of some genus five curve that is the intersection of three quadric hypersurfaces in $\mathbb{P}^4$. The curve $\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}$ is the same shape as the curve treated on [14] (with $m_0=b_2-1$, $m_1=-b_3$ and $m_2=-b_4$). Then we are going to apply this method to our curves. Let us write $\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}$ in the following form:

$$\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}} \,:\, \{X_k^2 = t^4-4b_kt^3+2(-b_2+2b_k+2b_2b_k)t^2-4b_2b_kt+b_2^2\}_{k=3,4}.$$

For $k\in\{3,4\}$ denote by:

l	$d_{k,l}$	$e_{k,l}$	$p_{k,l,\pm}(t)$
1	$b_k(b_k-1)$	$b_k(1-b_2)$	$t^2-2(b_k\pm\alpha_{k,1})t+b_2(-1+2(b_k\pm\alpha_{k,1}))$
2	$(b_k-1)(b_k-b_2)$	b_k-b_2	$t^2-2(b_k\pm\alpha_{k,2})t+b_2$
3	$b_k(b_k-b_2)$	0	$t^2-2(b_k\pm\alpha_{k,3})t-b_2+2(b_k\pm\alpha_{k,3})$

where $\alpha_{k,l}=\sqrt{d_{k,l}}$. Next, choose $l_3,l_4\in\{1,2,3\}$ and for any $k\in\{3,4\}$ denote by

- $\phi_k : E'_{(k)} \to E_{(k)}$ the 2-isogeny corresponding to the 2-torsion point $(e_{k,l_k},0)\in E_{(k)}(\mathbb{Q})$,

- $L = \mathbb{Q}(\alpha_{3,l_1}, \alpha_{4,l_2})$,
- $\mathcal{S}_L(\phi_k)$ a set of representatives in L of the image of the ϕ_k-Selmer group $\mathrm{Sel}(\phi_k)$ in $L^*/(L^*)^2$ via the natural map,
- $\widetilde{\mathcal{S}_L}(\phi_3)$ a set of representatives of $\mathrm{Sel}(\phi_3)$ modulo the subgroup generated by the image of $[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1]$ in this Selmer group,
- $\mathfrak{S} = \{\delta_3\delta_4 \;:\; \delta_3 \in \widetilde{\mathcal{S}_L}(\phi_3), \delta_4 \in \mathcal{S}_L(\phi_4)\} \subset \mathbb{Q}^*$,
- for any $\delta \in \mathfrak{S}$ and $s = (s_3, s_4) \in \{\pm\} \times \{\pm\}$ we define the genus one curve:

$$H_s^\delta : \delta z^2 = p_{3,l_3,s_3}(t)p_{4,l_4,s_4}(t).$$

Then we obtained the following fact:

$$\left\{ t \in \mathbb{P}^1(\mathbb{Q}) \;\middle|\; \begin{array}{c} \exists X_3, X_4 \in \mathbb{Q} \text{ such that} \\ (t, X_3, X_4) \in \mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}(\mathbb{Q}) \end{array} \right\}$$
$$\subseteq \bigcup_{\delta \in \mathfrak{S}} \left\{ t \in \mathbb{P}^1(\mathbb{Q}) \;\middle|\; \begin{array}{l} \exists w \in L \text{ such that } (t, w) \in H_s^\delta(L) \\ \text{for some } s \in \{\pm\} \times \{\pm\} \end{array} \right\}.$$

Note that in order to compute $\mathcal{C}^{a,q}_{\{n_0,n_1,n_i,n_j\}}(\mathbb{Q})$ we must find a pair $l_3, l_4 \in \{1, 2, 3\}$ such that for any $\delta \in \mathfrak{S}$ we can find $s \in \{\pm\} \times \{\pm\}$ where we can carry out all these computations to obtain the rational t-coordinates of $H_s^\delta(L)$. To work out this we must solve some problems. In practice all of them are solved by implementations in `Magma` [4]:

- $H_s^\delta(L) = \emptyset$? To answer this question we use the Bruin and Stoll's algorithm [9]. If the answer is yes, we have finished with δ and go for another element of $\mathfrak{S}$. Otherwise, we must find (by brute force) a point on $H_s^\delta(L)$.
- Once we have found a point on $H_s^\delta(L)$, we use it to create an L-isomorphism with its Jacobian $\mathrm{Jac}(H_s^\delta)$ and compute an upper bound for the rank r of the Mordell-Weil group of the elliptic curve $\mathrm{Jac}(H_s^\delta)(L)$.
- In the case where the rank $r \leq [L : \mathbb{Q}]$ we use the elliptic curve Chabauty algorithm (see [8]) to compute the t-coordinates of $H_s^\delta(L)$. For this purpose, we first must determine a sytem of generators of the Mordell-Weil group of $\mathrm{Jac}(H_s^\delta)(L)$.

Suppose that $\mathcal{S} = \{i, j, k, l\}$ then the curve $\mathcal{C}^{a,q}_{\mathcal{S}}$ has been defined by $\{d_i = d_j, d_i = d_k, d_i = d_l\}$. Note that we even may describe this curve by $\{d_{n_1} = d_{n_2}, d_{n_3} = d_{n_4}, d_{n_5} = d_{n_6}\}$ with $\{n_1, \dots, n_6\} = \{i, j, k, l\}$. There are 16 such descriptions if we do not take care on the order of the equations. That is, we can consider 16 models of $\mathcal{C}^{a,q}_{\mathcal{S}}$ of the form (1). The possible values of b_2, b_3, b_4 as a set appear at table 1. Then we parametrized the first conic and make the appropriate substitution on the other two conics. Therefore we have 48 different models of $\mathcal{C}^{a,q}_{\mathcal{S}}$ of the form (1) taking care on the order of the equations. In practice this is an important fact, since all the computations that we must carry out may work out only in a particular model, if any. Notice that we only consider the case when L is at most a quadratic field. The reason is because some of the computations are not well implemented for number fields of higher degree.

3. Proof of Theorem 1. Non-Symmetric case.

We are going to study when a non-symmetric arithmetic progression $a, a + q, \dots, a + (m - 1)q$ belongs to E_d. In particular $a \notin \{0, \pm q/2\}$. For this purpose we are going to use the translation given at the previous section with $\mathcal{S} = \{0, 1, \dots, m-1\}$. Notice that if $a + kq = 0$ then this case corresponds to the central

N	$\{b_2, b_3, b_4\}$	N	$\{b_2, b_3, b_4\}$	N	$\{b_2, b_3, b_4\}$	N	$\{b_2, b_3, b_4\}$
1	$s_{ij} s_{ik}, s_{il}$	2	s_{ji}, s_{jk}, s_{jl}	3	s_{ki}, s_{kj}, s_{kl}	4	s_{li}, s_{lj}, s_{lk}
5	r_{ij}, t_{ijk}, t_{ijl}	6	r_{ik}, t_{ikj}, t_{ikl}	7	r_{il}, t_{ilj}, t_{ilk}	8	r_{ji}, t_{jik}, t_{jil}
9	r_{jk}, t_{jki}, t_{jkl}	10	r_{jl}, t_{jli}, t_{jlk}	11	r_{ki}, t_{kij}, t_{kil}	12	r_{kj}, t_{kji}, t_{kjl}
13	r_{kl}, t_{kli}, t_{klj}	14	r_{li}, t_{lij}, t_{lik}	15	r_{lj}, t_{lji}, t_{ljk}	16	r_{lk}, t_{lki}, t_{lkj}

TABLE 1. Models for $\mathcal{C}^{a,q}_{\{i,j,k,l\}}$

symmetric case. If $a + kq \in \{\pm 1\}$ for some $k \in \mathcal{S}$, then we have $d_k = 1$ and therefore we can not use it for our purposes and we must use the curve $\mathcal{C}^{a,q}_{\mathcal{S}^*}$ where $\mathcal{S}^*$ is the set $\mathcal{S}$ removing such values of k. First we are going to assume that at most there is one value of $k \in \mathcal{S}$ satisfies $a + kq = 1$ or $a + kq = -1$. The other cases will be treated at the end of this section.

• $\#\mathcal{S}^* \leq 1$: these cases are particularly simple. If $a = \pm 1$ then the set $\mathcal{AP}_m(a, q)$ is described by $d \neq 1$ when $m = 1$ and by d_1 when $m = 2$. Meanwhile, d_0 describes the case $m = 1$ and $a \neq \pm 1$, and $m = 2$ and $a + q = \pm 1$.

Now, for the rest of the cases, that is when $\#\mathcal{S}^* > 1$, we have that there is a bijection between the sets $\mathcal{C}^{a,q}_{\mathcal{S}^*}(\mathbb{Q})$ and $\mathcal{AP}_m(q)$ for $m = \#\mathcal{S}$. We denote by:

$\mathcal{S}^*$	$\mathcal{C}^{a,q}_{\mathcal{S}^*}$	genus$(\mathcal{C}^{a,q}_{\mathcal{S}^*})$
$\{i, j\}$	$\mathcal{C}_{ij}(a, q)$	0
$\{i, j, k\}$	$\mathcal{E}_{ijk}(a, q)$	1
$\{i, j, k, l\}$	$\mathcal{D}_{ijkl}(a, q)$	5

Next table shows who is $\mathcal{C}^{a,q}_{\mathcal{S}^*}$ for each case.

	$m = 1$	$m = 2$	$m = 3$	$m = 4$	$m = 5$
$a = \pm 1$	$d \neq 1$	d_1	$\mathcal{C}_{12}(a, q)$	$\mathcal{E}_{123}(a, q)$	$\mathcal{D}_{1234}(a, q)$
$a + q = \pm 1$	d_0	d_0	$\mathcal{C}_{02}(a, q)$	$\mathcal{E}_{023}(a, q)$	$\mathcal{D}_{0234}(a, q)$
$a + 2q = \pm 1$		$\mathcal{C}_{01}(a, q)$	$\mathcal{C}_{01}(a, q)$	$\mathcal{E}_{013}(a, q)$	$\mathcal{D}_{0134}(a, q)$
$a + 3q = \pm 1$			$\mathcal{E}_{012}(a, q)$	$\mathcal{E}_{012}(a, q)$	$\mathcal{D}_{0124}(a, q)$
				$\mathcal{D}_{0123}(a, q)$	

We are going to split the proof depending on the cardinality of the set $\mathcal{S}^*$:

• $\mathcal{S}^* = \{i, j\}$: then the corresponding curve is the conic $\mathcal{C}_{ij}(a, q)$ with equation

$$\mathcal{C}_{ij}(a, q) : z_j^2 = s_{ij} w^2 + (1 - s_{ij}) z_i^2 .$$

This conic has been parametrized on the previous section by

$$[w : z_i : z_j] = [t^2 - 2t + s_{ij} : -t^2 + s_{ij} : t^2 - 2 s_{ij} t + s_{ij}],$$

therefore we have $\#\mathcal{AP}_m(q) = \infty$ when $s = \#\mathcal{S}$ and $\#\mathcal{S}^* = 2$. These cases correspond to $\mathcal{S} = \{0, 1\}$ and $a + kq \notin \{\pm 1\}$ for $k \in \{0, 1\}$ or $\mathcal{S} = \{0, 1, 2\}$ and $a + kq \in \{\pm 1\}$ for $k \in \{0, 1, 2\}$.

• $\mathcal{S}^* = \{i, j, k\}$: we have proved on the previous section that the corresponding curve is an elliptic curve that is $\mathbb{Q}$-isomorphic to the elliptic curve $\mathcal{E}_{ijk}(q)$ with Weierstrass model

$$\mathcal{E}_{ijk}(q) \,:\, y^2 = x(x + s_{ij} - s_{ik})(x + s_{ik}(s_{ij} - 1)),$$

and such that it has full 2-torsion defined over $\mathbb{Q}$ and the extra rational point $Q=(s_{ik}, s_{ij}s_{ik})$. Our first objective is to prove that Q is not a point of finite order for the cases

$$(i,j,k,a)\in\{(1,2,3,\pm1),(0,2,3,\pm1-q),(0,1,3,\pm1-2q),(0,1,2,\pm1-3q)\}.$$

Here we use Mazur's theorem. Then it is equivalent that Q has infinite order than nQ is not a point of order 2 for $n=1,2,3,4$. That is the y-coordinate of nQ, y_n, (that belongs to $\mathbb{Q}(q)$) is not 0. We have factorized the numerator and denominator of y_n for $n=1,2,3,4$ and we have obtained that the factors of degree one correspond to symmetric arithmetic progressions. Therefore we have proved that $\mathcal{E}_{ijk}(a,q)$ has positive rank for any (i,j,k,a) as above and any q such that do not correspond to a symmetric arithmetic progression. Same arguments may be applied for the case $(i,j,k)=(0,1,2)$ and any a,q. In this case, $y_n\in\mathbb{Q}(a,q)$ and therefore the factors of its numerator and denominator define plane affine curves. All the corresponding genus zero curves come from the polynomials $a, q, a+q, 2a+q, a+q\pm1, a+2q\pm1$. But we have assumed that those polynomials are different from zero. The genus one curves define elliptic curves of rank zero and therefore only a finite number of points (in fact, the corresponding points are related to symmetric arithmetic progressions). The rest of the curves are of genus greater than one, and therefore they have only a finite number of rational points.

In particular this finishes the proof of the statement $\#\mathcal{AP}_m(a,q)=\infty$ if $m\leq 3$, except for maybe a finite number of pairs (a,q).

• $\mathcal{S}^*=\{i,j,k,l\}$: in this case the corresponding curve is the genus five curve $\mathcal{D}_{ijkl}(a,q)$. Then, by Faltings' Theorem, $\#\mathcal{D}_{ijkl}(a,q)(\mathbb{Q})<\infty$. This proves that $\#\mathcal{AP}_m(a,q)<\infty$ when $s=\#\mathcal{S}$ and $\#\mathcal{S}^*=4$. These cases correspond to $\mathcal{S}=\{0,1,2,3,4\}$ and $a+kq\in\{\pm1\}$ for $k\in\{0,1,2,3\}$ or $\mathcal{S}=\{0,1,2,3\}$ and $a+kq\notin\{\pm1\}$ for $k\in\{0,1,2,3\}$.

Now we are going to give the proof when there are more than one value $k\in\mathcal{S}$ such that $a+kq\in\{\pm1\}$. Note that if $i,j\in\mathbb{Z}_{\geq0}$ such that $i<j$ satisfy $a+iq=-1$ and $a+jq=1$ then $a=(j+i)/(j-i)$ and $q=2/(j-i)$. Therefore, there are at most two possible values. The following table shows all those cases:

<table>
<tr><th>(i,j)</th><th>(a,q)</th><th>$m=1$</th><th>$m=2$</th><th>$m=3$</th><th>$m=4$</th><th>$m=5$</th><th>$m=6$</th></tr>
<tr><td>$(0,1)$</td><td>$(1,2)$</td><td colspan="6">Non-central symmetric arithmetic progression $(a,q)=(-1,2)$</td></tr>
<tr><td>$(0,2)$</td><td>$(1,1)$</td><td colspan="6">Central symmetric arithmetic progression $(a,q)=(0,1)$</td></tr>
<tr><td>$(0,3)$</td><td>$(1,2/3)$</td><td rowspan="2">$d\neq1$</td><td rowspan="2">d_1</td><td colspan="2">$\mathcal{C}_{12}(1,2/3)$</td><td>$\mathcal{E}_{124}(1,2/3)$</td><td>$\mathcal{D}_{1245}(1,2/3)$</td></tr>
<tr><td>$(0,4)$</td><td>$(1,1/2)$</td><td>$\mathcal{C}_{12}(1,1/2)$</td><td colspan="2">$\mathcal{E}_{123}(1,1/2)$</td><td>$\mathcal{D}_{1235}(1,1/2)$</td></tr>
<tr><td>$(1,2)$</td><td>$(3,2)$</td><td colspan="6">Non-central symmetric arithmetic progression $(a,q)=(-1,2)$</td></tr>
<tr><td>$(1,3)$</td><td>$(2,1)$</td><td colspan="6">Central symmetric arithmetic progression $(a,q)=(0,1)$</td></tr>
<tr><td>$(1,4)$</td><td>$(5/3,2/3)$</td><td rowspan="4">d_0</td><td>d_0</td><td>$\mathcal{C}_{02}(5/3,2/3)$</td><td colspan="2">$\mathcal{E}_{023}(5/3,2/3)$</td><td>$\mathcal{D}_{0235}(5/3,2/3)$</td></tr>
<tr><td>$(2,3)$</td><td>$(5,2)$</td><td colspan="2" rowspan="3">$\mathcal{C}_{01}(a,q)$</td><td>$\mathcal{C}_{01}(5,2)$</td><td>$\mathcal{E}_{014}(5,2)$</td><td>$\mathcal{D}_{0145}(5,2)$</td></tr>
<tr><td>$(2,4)$</td><td>$(3,1)$</td><td colspan="2">$\mathcal{E}_{013}(3,1)$</td><td>$\mathcal{D}_{0135}(3,1)$</td></tr>
<tr><td>$(3,4)$</td><td>$(7,2)$</td><td colspan="2">$\mathcal{E}_{012}(7,2)$</td><td>$\mathcal{D}_{0125}(7,2)$</td></tr>
</table>

The cases $(i,j)\in\{(0,1),(0,2),(1,2),(1,3)\}$ correspond to symmetric arithmetic progressions. The rest of the cases are going to be deal separately. We describe the first case in detail: Let be $(a,q)=(1,2/3)$. Then $\mathcal{AP}_m(1,2/3)$ is described by $d\neq1$ if $m=1$, by d_1 if $m=2$, by the conic $\mathcal{C}_{12}(1,2/3)$ if $m=3$ or $m=$

4, by $\mathcal{E}_{124}(1,2/3)$ if $m=5$ and by the genus five curve $\mathcal{D}_{1245}(1,2/3)$ if $m=6$. Then to prove the theorem for this specific case we only need to check that the above conic and elliptic curve have infinitely many points; since a genus five curve always has finitely many. For the conic is trivial since it has a rational point, and therefore infinitely many. For the elliptic curve it is enough to prove that the point $Q=(54/175,1458/21875)\in\mathcal{E}_{124}(1,2/3)(\mathbb{Q})$ is non-torsion. For this purpose we are going to use the Nagell-Lutz theorem. Then, we need to compute an integral model and we check if the coordinates of Q' (the image of the point Q in this integral model) or nQ', for some positive integer n, are not rational integers. An integral model is $y^2=x^3-107828175x-169430080750$ and $Q'=(16765,1653750)$, that has integral coordinates. But $2Q'=(143119/9,-39471328/27)$ does not. Therefore $\mathcal{E}_{124}(1,2/3)$ has infinitely many rational points.

The other cases work out similarly. Only the prove that the elliptic curve involved have positive rank is non trivial. The following table shows for each case, an integral model and the x-coordinate of nQ' for the first n such that nQ' has not integral coordinates.

(a,q)	integral model	n	$x(nQ')$
$(1,1/2)$	$y^2=x^3-1698765075x-15805306487250$	3	5714173479/2209
$(5/3,2/3)$	$y^2=x^3-17758025712x-853914488563584$	4	381665937/1156
$(5,2)$	$y^2=x^3-5530012992x-40473944856576$	3	2091682075560/19088161
$(3,1)$	$y^2=x^3-64092x-1772624$	1	4697/16
$(7,2)$	$y^2=x^3-178355952x-487934354304$	3	95604062772/5755201

Then we have proved the second and third items of theorem 1. For the last item we must compute all the rational points of some genus five curves. For this purpose we are going to apply the algorithm described on section 2. Let us start with the case $(a,q)=(1,2/3)$. Then the genus five curve is $\mathcal{D}_{1245}(1,2/3)$ and we choose the model $N=7$ from the table 1 with $b_2=2/3, b_3=250/81, b_4=20/21$, and the pair $(l_3,l_4)=(2,2)$. In this case $L=\mathbb{Q}(\sqrt{-6})$, $\mathfrak{S}=\{\pm1,\pm14,\pm26,\pm91\}$ and the following polynomials:

$$\begin{array}{ll} p_{3,2,+}(t)=t^2-32/3t+2/3, & p_{3,2,-}(t)=t^2-136/81t+2/3, \\ p_{4,2,+}(t)=t^2-2/21(20+\sqrt{-6})t+2/3, & p_{4,2,-}(t)=t^2-2/21(20-\sqrt{-6})t+2/3 \end{array}$$

Now for any $\delta\in\mathfrak{S}$, we must compute all the points $(t,w)\in H^{\delta}_{\pm,\pm}(\mathbb{Q}(\sqrt{-6}))$ with $t\in\mathbb{P}^1(\mathbb{Q})$ for some choice of the signs $s=(s_3,s_4)\in\{\pm\}\times\{\pm\}$ where

$$H^{\delta}_{s}\,:\,\delta w^2=p_{3,2,s_3}(t)\,p_{4,2,s_4}(t).$$

We have that $\mathrm{rank}_{\mathbb{Z}}\,H^{1}_{(-,+)}(\mathbb{Q}(\sqrt{-6}))=\mathrm{rank}_{\mathbb{Z}}\,H^{14}_{(+,+)}(\mathbb{Q}(\sqrt{-6}))=1$ therefore we can apply elliptic curve Chabauty to obtain the possible values of t. For $\delta=1$ (resp. $\delta=14$) we obtain $t=\infty$ and $t=0$ (resp. $t=1$ and $t=2/3$). For all of those values we obtain the trivial points $[1:\pm1:\pm1:\pm1:\pm1]\in\mathcal{D}_{1245}(1,2/3)(\mathbb{Q})$. For $\delta\in\{-1,-14,\pm26,\pm91\}$, we obtain $H^{\delta}_{(+,+)}(\mathbb{Q}(\sqrt{-6}))=\varnothing$ using Bruin and Stoll's algorithm [9].

The following table shows all the previous data, where at the last column appears if the corresponding points attached to t in the curve are trivial or not:

δ	s	$H_s^\delta(\mathbb{Q}(\sqrt{-6})) = \varnothing$?	$\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{-6}))$	t	trivial?
1	$(-,+)$	no	1	$0,\infty$	yes
-1	$(+,+)$	yes	$-$	$-$	$-$
14	$(+,+)$	no	1	$1, 2/3$	yes
-14	$(+,+)$	yes	$-$	$-$	$-$
26	$(+,+)$	yes	$-$	$-$	$-$
-26	$(+,+)$	yes	$-$	$-$	$-$
91	$(+,+)$	yes	$-$	$-$	$-$
-91	$(+,+)$	yes	$-$	$-$	$-$

$(i,j,k,l) = (1,2,4,5), (a,q) = (1,2/3), N = 7, (b_2,b_3,b_4) = (2/3, 250/81, 20/21), (l_3,l_4) = (2,2)$

Looking at the previous table, we obtain $\mathcal{D}_{1245}(1,2/3)(\mathbb{Q}) = \{[1 : \pm1 : \pm1 : \pm1 : \pm1]\}$; and therefore $\#\mathcal{AP}_m(1,2/3) = 0$ for any $m \geq 6$.

At the next four tables we show equivalent tables for the other cases.

δ	s	$H_s^\delta(\mathbb{Q}(\sqrt{-14})) = \varnothing$?	$\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{-14}))$	t	trivial?
1	$(-,+)$	no	1	∞	yes
-2	$(+,+)$	yes	$-$	$-$	$-$
-5	$(+,+)$	yes	$-$	$-$	$-$
10	$(+,+)$	yes	$-$	$-$	$-$

$(i,j,k,l) = (1,2,3,5), (a,q) = (1,1/2), N = 2, (b_2,b_3,b_4) = (3/28, 11/60, -7/20), (l_3,l_4) = (2,3)$

δ	s	$H_s^\delta(\mathbb{Q}(\sqrt{7})) = \varnothing$?	$\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{7}))$	t	trivial?
1	$(-,+)$	no	1	∞	yes
-5	$(+,+)$	yes	$-$	$-$	$-$

$(i,j,k,l) = (0,2,3,5), (a,q) = (5/3,2/3), N = 6, (b_2,b_3,b_4) = (49/54, 175/162, 175/54), (l_3,l_4) = (3,1)$

δ	s	$H_s^\delta(\mathbb{Q}(\sqrt{-1})) = \varnothing$?	$\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{-1}))$	t	trivial?
1	$(+,+)$	no	1	∞	yes
-7	$(+,-)$	yes	$-$	$-$	$-$

$(i,j,k,l) = (0,1,4,5), (a,q) = (5,2), N = 4, (b_2,b_3,b_4) = (-6/169, -5/338, 1/676), (l_3,l_4) = (2,3)$

δ	s	$H_s^\delta(\mathbb{Q}(\sqrt{385})) = \varnothing$?	$\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{385}))$	t	trivial?
1	$(-,+)$	no	1	$\infty, -1/20$	yes
21	$(+,+)$	yes	$-$	$-$	$-$
22	$(+,+)$	no	1	$0, 1$	yes
30	$(+,+)$	yes	$-$	$-$	$-$

$(i,j,k,l) = (1,2,3,5), (a,q) = (1,1/2), N = 2, (b_2,b_3,b_4) = (3/28, 11/60, -7/20), (l_3,l_4) = (2,3)$

This concludes the proof of theorem 1.

Note that our algorithm does not work in the case $\mathcal{D}_{0125}(7,2)(\mathbb{Q})$. A computer search similar to the ones on section 6 has been performed for the genus five curve $\mathcal{D}_{0125}(7,2)$. But only trivial points have been found.

4. Proof of Theorem 2. Central Symmetric case.

Same arguments as the ones used on previous section will be adapted to the central symmetric case. In this case $a = 0$, $\mathcal{S} = \{1, 2, \dots, m\}$ and the condition $a + kq \in \{\pm 1\}$ becomes $kq = 1$. Let $\mathcal{S}^*$ be the set $\mathcal{S}$ removing k.

If $\#\mathcal{S}^* \leq 1$ the set $\mathcal{S}_c\mathcal{AP}_{2s+1}(q)$ is described by the function d_1 when $s = 1$ and $q \neq 1$; by $d \neq 1$ if $(s, q) = (1, 1)$; by d_2 when $(s, q) = (2, 1)$ and by d_1 when $(s, q) = (2, 1/2)$.

If $\#\mathcal{S}^* \geq 2$, we use the the bijection between $\mathcal{C}^{0;q}_{\mathcal{S}^*}(\mathbb{Q})$ and $\mathcal{S}_c\mathcal{AP}_{2s+1}(q)$ for $s = \#\mathcal{S}$. Table 2 shows who is $\mathcal{C}^{0;q}_{\mathcal{S}^*}$ for each case.

q	$m=3$	$m=5$	$m=7$	$m=9$	$m=11$
1	$d \neq 1$	d_2	$\mathcal{C}_{23}(0,1)$	$\mathcal{E}_{234}(0,1)$	$\mathcal{D}_{2345}(0,1)$
$1/2$	d_1	d_1	$\mathcal{C}_{13}(0,1/2)$	$\mathcal{E}_{134}(0,1/2)$	$\mathcal{D}_{1345}(0,1/2)$
$1/3$		$\mathcal{C}_{12}(0,q)$	$\mathcal{C}_{12}(0,1/3)$	$\mathcal{E}_{124}(0,1/3)$	$\mathcal{D}_{1245}(0,1/3)$
$1/4$			$\mathcal{E}_{123}(0,q)$	$\mathcal{E}_{123}(0,1/4)$	$\mathcal{D}_{1235}(0,1/4)$
				$\mathcal{D}_{1234}(0,q)$	

Table 2. Moduli for $\mathcal{S}_c\mathcal{AP}_m(q)$

Now, if $\mathcal{S}^* = \{i, j\}$ the corresponding curve is the conic $\mathcal{C}_{ij}(0, q)$ that has infinite number of points. Therefore we have $\#\mathcal{S}_c\mathcal{AP}_{2s+1}(q) = \infty$ when $s = \#\mathcal{S}$ and $\#\mathcal{S}^* = 2$. These cases correspond to $\mathcal{S} = \{1, 2, 3\}$ and $q \in \{1, 1/2, 1/3\}$ or $\mathcal{S} = \{1, 2\}$ and $q \notin \{1, 1/2\}$.

The case $\mathcal{S}^* = \{i, j, k\}$ corresponds to the elliptic curve $\mathcal{E}_{ijk}(0, q)$ which has full 2-torsion defined over $\mathbb{Q}$ and the extra rational point $Q = (s_{ik}, s_{ij}s_{ik})$. Our objective is to prove that Q is not a point of finite order for the cases $(i, j, k, q) \in \{(2, 3, 4, 1), (1, 3, 4, 1/2), (1, 2, 4, 1/3)\}$ and $(i, j, k) = (1, 2, 3)$ for any $q \in \mathbb{Q}_{>0}$, $q \notin \{1, 1/2, 1/3\}$. The first attempt is to use the Nagell-Lutz theorem. For this purpose, we compute an integral model of $\mathcal{E}_{ijk}(0, q)$ and we check if the coordinates of Q' (the image of the point Q in this integral model) are not rational integers. The following table shows for each case, an integral model and the x-coordinate of nQ' for the first n such that nQ' has not integral coordinates.

(i,j,k,q)	integral model	n	$x(nQ')$
$(2,3,4,1)$	$y^2 = x^3 - 25444800x - 35897472000$	2	$185721/16$
$(1,3,4,1/2)$	$y^2 = x^3 - 11697075x + 15251172750$	3	$4532055/961$
$(1,2,4,1/3)$	$y^2 = x^3 - 308700x - 55566000$	1	$-4095/16$

Therefore if $(i, j, k, q) \in \{(2, 3, 4, 1), (1, 3, 4, 1/2), (1, 2, 4, 1/3)\}$ we have obtained that the point Q is not of finite order.

Note that this procedure does not work for the case $(i, j, k) = (1, 2, 3)$ with $q \in \mathbb{Q}_{>0}$, $q \notin \{1, 1/2, 1/3\}$. By Mazur's theorem, Q has infinite order if and only if nQ is not a point of order 2 for $n = 1, 2, 3, 4$. That is the y-coordinate of nQ, y_n, (that belongs to $\mathbb{Q}(q)$) is not 0. We have factorized the numerator and denominator of y_n for $n = 1, 2, 3, 4$ and we have obtained that they have not any root $q \in \mathbb{Q}_{>0}$ with $q \notin \{1, 1/2, 1/3\}$. Therefore we have proved that $\mathcal{E}_{ijk}(0, q)$ has positive rank for any (i, j, k, q) as above. This proves $\#\mathcal{S}_c\mathcal{AP}_{2s+1}(q) = \infty$ when $s = \#\mathcal{S}$ and

$\#\mathcal{S}^* = 3$. These cases correspond to $\mathcal{S} = \{1,2,3,4\}$ and $q \in \{1, 1/2, 1/3, 1/4\}$ or $\mathcal{S} = \{1,2,3\}$ and $q \notin \{1, 1/2, 1/3, 1/4\}$.

In particular this finishes the proof of the statement $\#\mathcal{S}_c\mathcal{AP}_7(q) = \infty$ for any $q \in \mathbb{Q}_{>0}$.

Finally the case $\mathcal{S}^* = \{i,j,k,l\}$ corresponding to the genus five curve $\mathcal{D}_{ijkl}(0,q)$ wich satisfies $\#\mathcal{D}_{ijkl}(0,q)(\mathbb{Q}) < \infty$. This proves that $\#\mathcal{S}_c\mathcal{AP}_{2s+1}(q) < \infty$ when $s = \#\mathcal{S}$ and $\#\mathcal{S}^* = 4$. These cases correspond to $\mathcal{S} = \{1,2,3,4,5\}$ and $q \in \{1, 1/2, 1/3, 1/4\}$ or $\mathcal{S} = \{1,2,3,4\}$ and $q \notin \{1, 1/2, 1/3, 1/4\}$. This concludes the proof of: $\#\mathcal{S}_c\mathcal{AP}_9(q) = \infty$ if and only if $q \in \{1, 1/2, 1/3, 1/4\}$ and $\#\mathcal{S}_c\mathcal{AP}_m(q) < \infty$ for $m \geq 11$ and any $q \in \mathbb{Q}_{>0}$.

The remaining of this section is devoted to prove that $\#\mathcal{S}_c\mathcal{AP}_m(q) = 0$ if $q \in \{1, 1/2, 1/3, 1/4\}$ for $m \geq 11$. Note that it is enough to prove it for $m = 11$. In other words, for $\mathcal{S} = \{1,2,3,4,5\}$ and $q \in \{1, 1/2, 1/3, 1/4\}$ we are going to prove that $\mathcal{C}^{0,q}_{\mathcal{S}^*}(\mathbb{Q}) = \{[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1]\}$. For this purpose we are going to apply the algorithm described on section 2.

The following four tables include the data related to the computation of all rational points of the curves $\mathcal{D}_{ijkl}(0,q)(\mathbb{Q})$ with $(i,j,k,l,q) \in \{(2,3,4,5,1), (1,3,4,5,1/2), (1,2,4,5,1/3), (1,2,3,5,1/4)\}$. In all these cases we have $\mathcal{D}_{ijkl}(0,q) = \{[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1]\}$.

δ	s	$H^\delta_s(\mathbb{Q}(\sqrt{-7})) = \varnothing$?	$\mathrm{rank}_{\mathbb{Z}}\, H^\delta_s(\mathbb{Q}(\sqrt{-7}))$	t	trivial?
1	$(+,+)$	no	1	∞	yes
-1	$(+,+)$	no	1	1	yes
10	$(+,+)$	yes	$-$	$-$	$-$
-10	$(+,+)$	yes	$-$	$-$	$-$

$(i,j,k,l) = \{2,3,4,5\}, q = 1, N = 11, (b_2, b_3, b_4) = (-4, 7/32, -3/32), (l_3, l_4) = (1,2)$

Notice that the previous table answer one of Moody's questions. We have $\#\mathcal{S}_c\mathcal{AP}_m(1) = 0$ for any $m \geq 11$, since $\mathcal{D}_{2345}(0,1)(\mathbb{Q}) = \{[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1]\}$.

δ	s	$H^\delta_s(\mathbb{Q}(\sqrt{14})) = \varnothing$?	$\mathrm{rank}_{\mathbb{Z}}\, H^\delta_s(\mathbb{Q}(\sqrt{14}))$	t	trivial?
1	$(+,-)$	no	1	∞	yes
2	$(+,+)$	yes	$-$	$-$	$-$
-5	$(+,+)$	yes	$-$	$-$	$-$
-10	$(+,+)$	yes	$-$	$-$	$-$

$(i,j,k,l) = \{1,3,4,5\}, q = 1/2, N = 3, (b_2, b_3, b_4) = (-3/25, 32/25, -64/125), (l_3, l_4) = (1,3)$

δ	s	$H^\delta_s(\mathbb{Q}(\sqrt{21})) = \varnothing$?	$\mathrm{rank}_{\mathbb{Z}}\, H^\delta_s(\mathbb{Q}(\sqrt{21}))$	t	trivial?
1	$(+,+)$	no	1	$\infty, 27/25$	yes
-1	$(+,+)$	yes	$-$	$-$	$-$
6	$(+,+)$	yes	$-$	$-$	$-$
-6	$(+,+)$	yes	$-$	$-$	$-$

$(i,j,k,l) = \{1,2,4,5\}, q = 1/3, N = 3, (b_2, b_3, b_4) = (27/25, 189/125, -81/175), (l_3, l_4) = (1,1)$

δ	s	$H_s^\delta(\mathbb{Q}(\sqrt{105}))=\varnothing$?	$\mathrm{rank}_\mathbb{Z}\, H_s^\delta(\mathbb{Q}(\sqrt{105}))$	t	trivial?
1	$(+,-)$	no	1	∞	yes
6	$(+,+)$	yes	–	–	–

$(i,j,k,l)=\{1,2,3,5\}, q=1/4, N=1, (b_2,b_3,b_4)=(128/3,-4,-128/7), (l_3,l_4)=(3,2)$

These computations conclude the proof of theorem 2.

5. Proof of Theorem 3. Non-Central Symmetric case.

Let us use the same arguments again. In this case we choose $a=-q/2$, $\mathcal{S}=\{1,2,\dots,m\}$ and the condition $a+kq\in\{\pm1\}$ becomes $(2k-1)q=2$. Let be $\mathcal{S}^*$ the set $\mathcal{S}$ removing k.

If $\#\mathcal{S}^*\leq 1$ the set $\mathcal{S}_{nc}\mathcal{AP}_m(q)$ is described by the function d_1 when $m=2$ and $q\neq 2$; by $d\neq 1$ if $(m,q)=(2,2)$; by d_2 when $(m,q)=(4,2)$ and by d_1 when $(m,q)=(4,2/3)$.

q	$m=2$	$m=4$	$m=6$	$m=8$	$m=10$
2	$d\neq 1$	d_2	$\mathcal{C}_{23}(-1,2)$	$\mathcal{E}_{234}(-1,2)$	$\mathcal{D}_{2345}(-1,2)$
2/3	d_1	d_1	$\mathcal{C}_{13}(-1/3,2/3)$	$\mathcal{E}_{134}(-1/3,2/3)$	$\mathcal{D}_{1345}(-1/3,2/3)$
2/5		$\mathcal{C}_{12}(-q/2,q)$	$\mathcal{C}_{12}(-1/5,2/5)$	$\mathcal{E}_{124}(-1/5,2/5)$	$\mathcal{D}_{1245}(-1/5,2/5)$
2/7			$\mathcal{E}_{123}(-q/2,q)$	$\mathcal{E}_{123}(-1/7,2/7)$	$\mathcal{D}_{1235}(-1/7,2/7)$
				$\mathcal{D}_{1234}(-q/2,q)$	

Table 3. Moduli for $\mathcal{S}_{nc}\mathcal{AP}_m(q)$

If $\#\mathcal{S}^*=2$, then $\mathcal{S}_{nc}\mathcal{AP}_{2s}(q)$ is parametrized by a conic with infinite rational points. Therefore we have $\#\mathcal{S}_{nc}\mathcal{AP}_{2s}(q)=\infty$ when $s=\#\mathcal{S}$ and $\#\mathcal{S}^*=2$. These cases correspond to $\mathcal{S}=\{1,2,3\}$ and $q\in\{2,2/3,2/5\}$ or $\mathcal{S}=\{1,2\}$ and $q\notin\{2,2/3\}$.

Now, the elliptic curve $\mathcal{E}_{ijk}(-q/2,q)$ parametrized the case when $\mathcal{S}^*=\{i,j,k\}$. This elliptic curve has all the 2-torsion points defined over $\mathbb{Q}$ and the extra rational point $Q=(s_{ik},s_{ij}s_{ik})$. Using Nagell-Lutz we proved that Q has infinite order for the cases $(i,j,k,q)\in\{(2,3,4,2),(1,3,4,2/3),(1,2,4,2/5)\}$. First we compute a suitable integral model of $\mathcal{E}_{ijk}(-q/2,q)$. Next table shows for each case the corresponding integral model and the x-coordinate of nQ' for the first n such that nQ' has not integral coordinates (where Q' is the image of Q in this model):

$\{i,j,k,q\}$	integral model	n	$x(nQ')$
$\{2,3,4,2\}$	$y^2=x^3-22427712x-33269059584$	3	2550847992/151321
$\{1,3,4,2/3\}$	$y^2=x^3-735300x+242352000$	2	18649/36
$\{1,2,4,2/5\}$	$y^2=x^3-4615488x-3696371712$	2	109761/25

The proof that Q has infinite order in the case $(i,j,k,a,q)=(1,2,3,-q/2,q)$ with $q\notin\{2,2/3,2/5\}$ is analogous to the case $(i,j,k,a,q)=(1,2,3,-0,q)$ with $q\notin\{1,1/2,1/3\}$ treated on the proof of theorem 2. This proves that $\#\mathcal{S}_{nc}\mathcal{AP}_{2s}(q)=\infty$ when $s=\#\mathcal{S}$ and $\#\mathcal{S}^*=3$. These cases correspond to $\mathcal{S}=\{1,2,3,4\}$ and $q\in\{2,2/3,2/5,2/7\}$ or $\mathcal{S}=\{1,2,3\}$ and $q\notin\{2,2/3,2/5,2/7\}$. Moreover, this concludes that $\#\mathcal{S}_{nc}\mathcal{AP}_6(q)=\infty$ for any $q\in\mathbb{Q}_{>0}$.

Finally, the genus five curve $\mathcal{D}_{ijkl}(-q/2,q)$ corresponds to the case $\mathcal{S}^* = \{i,j,k,l\}$. Now, since $\#\mathcal{D}_{ijkl}(-q/2,q)(\mathbb{Q}) < \infty$ we obtain that $\#\mathcal{S}_{nc}\mathcal{AP}_{2s}(q) < \infty$ when $s = \#\mathcal{S}$ and $\#\mathcal{S}^* = 4$. These cases correspond to $\mathcal{S} = \{1,2,3,4,5\}$ and $q \in \{2, 2/3, 2/5, 2/7\}$ or $\mathcal{S} = \{1,2,3,4\}$ and $q \notin \{2, 2/3, 2/5, 2/7\}$. This concludes the proof of: $\#\mathcal{S}_{nc}\mathcal{AP}_8(q) = \infty$ if and only if $q \in \{2, 2/3, 2/5, 2/7\}$ and $\#\mathcal{S}_{nc}\mathcal{AP}_m(q) < \infty$ for $m \geq 10$ and any $q \in \mathbb{Q}_{>0}$.

The following four tables include the data related to the computation of all rational points of the curves $\mathcal{D}_{ijkl}(-q/2,q)$ with $(i,j,k,l,q) \in \{(2,3,4,5,2), (1,3,4,5,2/3), (1,2,4,5,2/5), (1,2,3,5,2/7)\}$. In all these cases we have $\mathcal{D}_{ijkl}(-q/2,q)(\mathbb{Q}) = \{[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1]\}$.

δ	s	$H_s^\delta(\mathbb{Q}(\sqrt{15})) = \varnothing$?	$\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{15}))$	t	trivial?
1	$(+,+)$	no	1	∞	yes
-1	$(+,+)$	yes	$-$	$-$	$-$
6	$(+,+)$	no	1	1	yes
-6	$(+,+)$	yes	$-$	$-$	$-$

$(i,j,k,l) = \{2,3,4,5\}, a = -1, q = 2, N = 9, (b_2,b_3,b_4) = (7/5, 50, -4), (l_3,l_4) = (2,3)$

δ	s	$H_s^\delta(\mathbb{Q}(\sqrt{10})) = \varnothing$?	$\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{10}))$	t	trivial?
1	$(+,-)$	no	1	$\infty, 0$	yes
-6	$(+,+)$	yes	$-$	$-$	$-$

$(i,j,k,l) = \{1,3,4,5\}, a = -1/3, q = 2/3, N = 2, (b_2,b_3,b_4) = (7/25, 27/25, 27/125), (l_3,l_4) = (2,2)$

δ	s	$H_s^\delta(\mathbb{Q}(\sqrt{21})) = \varnothing$?	$\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{21}))$	t	trivial?
1	$(+,+)$	no	1	∞	yes
-1	$(+,+)$	yes	$-$	$-$	$-$
6	$(+,+)$	yes	$-$	$-$	$-$
-6	$(+,+)$	yes	$-$	$-$	$-$

$(i,j,k,l) = \{1,2,4,5\}, a = -1/5, q = 2/5, N = 6, (b_2,b_3,b_4) = (5/7, 1/50, -1/4), (l_3,l_4) = (2,3)$

δ	s	$H_s^\delta(\mathbb{Q}(\sqrt{7})) = \varnothing$?	$\operatorname{rank}_{\mathbb{Z}} H_s^\delta(\mathbb{Q}(\sqrt{7}))$	t	trivial?
1	$(-,+)$	no	1	$\infty, 0$	yes
2	$(+,+)$	yes	$-$	$-$	$-$
5	$(+,+)$	yes	$-$	$-$	$-$
10	$(+,+)$	yes	$-$	$-$	$-$

$(i,j,k,l) = \{1,2,3,5\}, a = -1/7, q = 2/7, N = 1, (b_2,b_3,b_4) = (245/2, -49/5, -49), (l_3,l_4) = (2,2)$

This concludes the proof of theorem 3.

6. Some computations

We would like to find an arithmetic progression on an Edwards curve as large as possible. It seems natural to look for symmetric ones since fewer restrictions appear. Then we performed a computer search on `Magma` to find a non-trivial rational point P of height $H(P) \leq 10^6$ in the curve $\mathcal{D}_{1234}(0,q)$ or in the curve $\mathcal{D}_{1234}(-q/2,q)$ for positive rationals q of height $H(q) \leq 100$ and $q \notin \{1, 1/2, 1/3, 1/4\}$ or $q \notin \{2, 2/3, 2/5, 2/7\}$ respectively. There are 6087 such q's. We have used the following models for $\mathcal{D}_{1234}(0,q)$ and $\mathcal{D}_{1234}(-q/2,q)$:

$$\mathcal{D}_{1234}(0,q)\ :\ \left\{\begin{array}{lcl} 3X_0^2+4(q^2-1)X_1^2+(1-4q^2)X_2^2 & = & 0,\\ 8X_0^2+9(q^2-1)X_1^2+(1-9q^2)X_3^2 & = & 0,\\ 15X_0^2+16(q^2-1)X_1^2+(1-16q^2)X_4^2 & = & 0,\end{array}\right.$$

$$\mathcal{D}_{1234}(-q/2,q)\ :\ \left\{\begin{array}{lcl} 32X_0^2+9(q^2-4)X_1^2+(4-9q^2)X_2^2 & = & 0,\\ 96X_0^2+25(q^2-4)X_1^2+(4-25q^2)X_3^2 & = & 0,\\ 192X_0^2+49(q^2-4)X_1^2+(4-49q^2)X_4^2 & = & 0.\end{array}\right.$$

This search has not found such a rational point. On the other hand, using the same techniques as the ones used on the proof of the last item of theorems 1, 2 and 3, we are able to prove that $\#\mathcal{D}_{1234}(0,q)=16$ for

$$q\in\left\{\begin{array}{c} 19/11, 11/13, 49/46, 13/3, 3/2, 3/7, 2, 11/43, 1/11,\\ 7/11, 1/8, 1/7, 1/6, 8/17, 1/5, 11/38, 5/17, 2/3, 11/37,\\ 7/13, 59/61, 29/53, 3/4, 11/19, 3/8, 37/95, 11/28\end{array}\right\},$$

and $\#\mathcal{D}_{1234}(-q/2,q)=16$ for

$$q\in\left\{\begin{array}{c} 2/9, 22/13, 14, 22/7, 14/11, 2/35, 6/7, 22/25, 34/19,\\ 2/17, 2/15, 22/73, 62/33, 2/13, 38/35, 10/7, 34/49, 22/31,\\ 26/21, 10/23, 34/77, 14/19, 26/11, 38/77, 22/43, 6/11\end{array}\right\},$$

Then for the corresponding list we have proved $\#\mathcal{S}_c\mathcal{AP}_9(q)=0$ and $\#\mathcal{S}_{nc}\mathcal{AP}_8(q)=0$ respectively.

Acknowledgement: We would like to thank to Nils Bruin, Luis Dieulefait and Xevi Guitart for useful discussion meanwhile the paper was written and José M. Tornero, who read the earlier versions of this paper carefully.

References

[1] A. Alvarado. Arithmetic progressions on quartic elliptic curves. *Ann. Math. Inform.*, 37:3–6, 2010.

[2] A. Alvarado. Arithmetic progressions in the y–coordinates on certain elliptic curves. In F. Luca and P. Stanica, editors, *Aportaciones Matemáticas, Investigación 20: Proceedings of the Fourteenth International Conference on Fibonacci Numbers*, pages 1–9. Sociedad Matemática Mexicana, 2011.

[3] E. Bombieri, A. Granville, and J. Pintz. Squares in arithmetic progressions. *Duke Math. J.*, 66(3):369–385, 1992.

[4] W. Bosma, J. Cannon, C. Fieker, and A. Steel, editors. *Handbook of Magma functions, Edition 2.19.* http://magma.maths.usyd.edu.au/magma, 2012.

[5] A. Bremner. Some special curves of genus 5. *Acta Arith.*, 79(1):41–51, 1997.

[6] A. Bremner. On arithmetic progressions on elliptic curves. *Experiment. Math.*, 8(4):409–413, 1999.

[7] A. Bremner, J. H. Silverman, and N. Tzanakis. Integral points in arithmetic progression on $y^2=x(x^2-n^2)$. *J. Number Theory*, 80(2):187–208, 2000.

[8] N. Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[9] N. Bruin and M. Stoll. Two-cover descent on hyperelliptic curves. *Math. Comp.*, 78(268):2347–2370, 2009.

[10] G. Campbell. A note on arithmetic progressions on elliptic curves. *J. Integer Seq.*, 6(1):Article 03.1.3, 5 pp. (electronic), 2003.

[11] C. Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[12] I. García-Selfa and J. M. Tornero. Searching for simultaneous arithmetic progressions on elliptic curves. *Bull. Austral. Math. Soc.*, 71(3):417–424, 2005.

[13] I. García-Selfa and J. M. Tornero. On simultaneous arithmetic progressions on elliptic curves. *Experiment. Math.*, 15(4):471–478, 2006.

[14] E. González-Jiménez and X. Xarles. On a conjecture of Rudin on squares in arithmetic progression. arXiv: 1301.5122, 2013.

[15] J.-B. Lee and W. Y. Vélez. Integral solutions in arithmetic progression for $y^2 = x^3 + k$. *Period. Math. Hungar.*, 25(1):31–49, 1992.

[16] A. J. MacLeod. 14-term arithmetic progressions on quartic elliptic curves. *J. Integer Seq.*, 9(1):Article 06.1.2, 4 pp. (electronic), 2006.

[17] S. P. Mohanty. On consecutive integer solutions for $y^2 - k = x^3$. *Proc. Amer. Math. Soc.*, 48:281–285, 1975.

[18] D. Moody. Arithmetic progressions on Edwards curves. *J. Integer Seq.*, 14(1):Article 11.1.7, 4, 2011.

[19] D. Moody. Arithmetic progressions on Huff curves. *Ann. Math. Inform.*, 38:111–116, 2011.

[20] R. Schwartz, J. Solymosi, and F. de Zeeuw. Simultaneous arithmetic progressions on algebraic curves. *Int. J. Number Theory*, 7(4):921–931, 2011.

[21] B. K. Spearman. Arithmetic progressions on congruent number elliptic curves. *Rocky Mountain J. Math.*, 41(6):2033–2044, 2011.

[22] M. Ulas. A note on arithmetic progressions on quartic elliptic curves. *J. Integer Seq.*, 8(3):Article 05.3.1, 5 pp. (electronic), 2005.

Universidad Autónoma de Madrid, Departamento de Matemáticas and Instituto de Ciencias Matemáticas (ICMat), Madrid, Spain

E-mail address: enrique.gonzalez.jimenez@uam.es

URL: http://www.uam.es/enrique.gonzalez.jimenez